

ABSTRACT

A system and method for the identification of users and objects using biometric techniques is disclosed. This invention describes a biometric based identification and authorization systems which do not require the incorporation of an on-line database of stored complete biometrics for the security infrastructure. In order to remove the connectivity requirements, an off-line biometric system is achieved by incorporating an identity verification template (IVT) on a storage device / token (e.g., magnetic strip or smart-card) during the user's registration which provides for a reliable storage medium; however, there are no security requirements required of the token even to protect the privacy of the stored biometric. The IVT does not contain complete information of the user's biometric but allows for the verification of the user when that user later provides a biometric reading. To deal with errors that may be introduced into later scans of the biometric (for example at the time of verification) error correcting techniques, well known in the art of communication and error control systems, are incorporated into the system. The system is also usable in the online model. Moreover, it may also be used to enable cryptographic operations by being used to partially compose or encrypt private keys for cryptographic operation.